intusdata

Regelung zur Auftragsdatenverarbeitung

1. September 2023

Diese Regelung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem Vertragsverhältnis von Intus Data mit dem Kunden ergeben. Massgebend sind insbesondere die gesetzlichen Bestimmungen: des schweizerischen Datenschutzgesetzes (DSG) und die Verordnung zum Datenschutzgesetz (VDSG). Diese Regelung findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen durch Intus Data personenbezogene Daten ("Daten") des Kunden verarbeitet werden.

1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

Die Laufzeit dieser Regelung richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Regelung nicht darüberhinausgehende Verpflichtungen ergeben.

Intus Data verarbeitet personenbezogene Daten des Kunden als Auftragsdatenverarbeiter in den folgenden Fällen:

- Bei der Migration von Daten aus externen Systemen in die Ziellösung gemäss einem Kundenauftrag. In diesem Fall werden personenbezogene Daten nur soweit verarbeitet, wie der Kunde diese zur Migration in die Ziellösung vorsieht und an Intus Data anliefert (z.B. Personendaten über Mitarbeitende des Kunden);
- Bei einem Auftrag zur Aufbewahrung einer Kopie der Kundendatenbank (dies erfordert einen separaten Auftrag des Kunden) zu Test- oder Supportzwecken. In diesem Fall werden personenbezogene Daten bearbeitet, die durch den Kunden in Kundendatenbank gespeichert wurden (z.B. Personendaten über Mitarbeitende des Kunden);
- Beim Intus Data Cloud Abo (Treuhandportal), bei dem Intus Data im Kundenauftrag die Software betreibt werden personenbezogene Daten bearbeitet, die durch den Kunden in der durch Intus Data bereitgestellten Datenbank gespeichert werden (z.B. Personendaten über Mitarbeitende des Kunden).

2 Anwendungsbereich und Verantwortlichkeit

Intus Data verarbeitet personenbezogene Daten im Auftrag des Kunden und nach seinen Weisungen. Der Kunde ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze für die Rechtmässigkeit der Datenverarbeitung verantwortlich ("Verantwortlicher" im Sinne des Art. 5 lit. j. DSG).

Die Weisungen werden durch den Vertrag festgelegt. Weisungen des Kunden, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt und sind kostenpflichtig.

3 Pflichten von Intus Data

Intus Data darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Kunden verarbeiten, ausser es liegt ein Rechtfertigungsgrund vor gemäss Art. 9 Abs. 4 DSG. Intus Data informiert den Kunden unverzüglich, wenn Intus Data der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstösst. Intus Data darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Kunden bestätigt oder abgeändert wurde.

Intus Data wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Intus Data wird technische und organisatorische Massnahmen zum angemessenen Schutz der Daten des Kunden treffen, die den Anforderungen des DSG (Art. 8 DSG) genügen. Sie müssen die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

Intus Data unterstützt soweit vereinbart und gegen gesonderte Vergütung den Kunden im Rahmen ihrer Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche von betroffenen Personen gem. dem 4. Kapitel des DSG sowie bei der Einhaltung der in Art. 24 DSG und 25 DSG genannten Pflichten.

Intus Data gewährleistet, dass es den mit der Verarbeitung der Daten des Kunden befassten Mitarbeitern und andere für Intus Data tätigen Personen untersagt ist, die Daten ausserhalb der Weisung zu verarbeiten. Ferner gewährleistet Intus Data, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

Intus Data unterrichtet den Kunden unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Kunden bekannt werden. Intus Data trifft die erforderlichen Massnahmen zur Sicherung der Daten und zur

Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Kunden ab.

Intus Data nennt dem Kunden den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

Intus Data gewährleistet, ihre Pflichten nach Art. 1 ff. VDSG nachzukommen, ein Verfahren zur regelmässigen Überprüfung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

Intus Data berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Kunde dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt Intus Data die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Kunden oder gibt diese Datenträger an den Kunden zurück. Diese Leistungen sind gesondert zu vergüten.

Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Kunden entweder herauszugeben oder zu löschen.

Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich etwaiger Ansprüche gemäss den anwendbaren Bestimmungen des schweizerischen Rechts, verpflichtet sich Intus Data den Kunden bei der Abwehr des Anspruches im Rahmen ihrer Möglichkeiten zu unterstützen. Diese Leistungen sind gesondert zu vergüten.

4 Pflichten des Kunden

Der Kunde hat Intus Data unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmässigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach den anwendbaren Bestimmungen des schweizerischen Rechts gilt Abschnitt 3 Abs. 10 dieses Dokumentes entsprechend.

Der Kunde nennt Intus Data den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an Intus Data, wird Intus Data die betroffene Person an den Kunden verweisen. Intus Data leitet den Antrag der betroffenen Person unverzüglich an den Kunden weiter. Intus Data haftet nicht, wenn das Ersuchen der betroffenen Person vom Kunden nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6 Nachweismöglichkeiten

Intus Data weist dem Kunden auf Aufforderung die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

Sollten im Einzelfall Inspektionen durch den Kunden erforderlich sein, muss der Kunde dafür einen anerkannten Datenschutzexperten beauftragen. Die Prüfung durch den Datenschutzexperten ist zu den üblichen Geschäftszeiten durchzuführen unter Berücksichtigung einer angemessenen Vorlaufzeit. Intus Data darf diese von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Massnahmen abhängig machen. Sollte der durch den Kunden beauftragte Prüfer in einem Wettbewerbsverhältnis zu Intus Data stehen, hat Intus Data gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf Intus Data eine Vergütung verlangen.

Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Kunden eine Inspektion vornehmen, gilt grundsätzlich der vorherige Absatz entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt.

7 Subunternehmer (weitere Auftragsverarbeiter)

Der Einsatz von Subunternehmern, ausgenommen Tochtergesellschaften von Intus Data, als weiteren Auftragsdatenverarbeiter ist nur zulässig, wenn der Kunde vorher zugestimmt hat.

Ausgenommen davon ist die Verarbeitung von Daten im Rahmen des durch Intus Data vermittelten Cloud Abos (z.B. Vertec Cloud Abo) und dem deren Webaccess Services.

Intus Data arbeitet mit Subunternehmern zusammen, welche hier aufgeführt sind:
https://www.Intusdata.ch/ch/sublieferanten/.

Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn Intus Data weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Intus Data wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um

angemessene Datenschutz- und Informationssicherheitsmassnahmen zu gewährleisten.

Erteilt Intus Data Aufträge an Subunternehmer, so obliegt es Intus Data, ihre datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Intus Data ist berechtigt, ohne die explizite Zustimmung des Kunden die Subunternehmer auszutauschen, falls die neuen Subunternehmer ein gleiches oder höheres Niveau an Datenschutz gewährleisten.

8 Informationspflichten, Schriftformklausel, Rechtswahl

Sollten die Daten des Kunden bei Intus Data durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet werden, so hat Intus Data den Kunden unverzüglich darüber zu informieren. Intus Data wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschliesslich beim Kunden liegen.

Änderungen und Ergänzungen dieser Regelung und aller ihrer Bestandteile – einschliesslich etwaiger Zusicherungen seitens Intus Data – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9 Haftung und Schadenersatz

Der Kunde und Intus Data haften gegenüber betroffenen Personen entsprechend den anwendbaren Bestimmungen des schweizerischen Rechts.

Übersicht über technische und organisatorische Massnahmen

10 Grundsätze, IT-Grundschutz

Das Informationssicherheits-Managementsystem der Intus Data AG misst dem Schutz der IT-Infrastruktur und der Ausbildung und Bewusstseinsbildung der Mitarbeitenden bez. den Bedrohungen der Informationssicherheit eine hohe Bedeutung zu.

Den folgenden Themenblöcken wird dabei eine erhöhte Wichtigkeit beigemessen:

Schutz der Client-Infrastruktur. Eine grosse Bedrohung für die Informationssicherheit geht von Arbeitsplatzrechnern und Notebooks der Mitarbeitenden aus. Dem Schutz dieser Infrastruktur misst Intus Data einen sehr hohen Stellenwert bei. Schutzmassnahmen beinhalten u. a.: Endpoint Detection & Response Lösung (XDR), Virenscanner, Verschlüsselung der Harddisks, Patchmanagement-Systeme inklusive automatischem Monitoring und Reporting, Härtung der Systeme gegen Angriffe über unnötig offene Ports. Zugriffschutz mittels 2-Factor-Authentication (DuoSecurity). Zum Schutz der Client-Infrastruktur gehört auch Förderung des Bewusstseins der Mitarbeitenden bezüglich der Risiken bez. Malware und Social Engineering.

Geo-redundantes, automatisiertes Backupkonzept mit verschlüsselter Datenübermittlung in einen ehemaligen Militärbunker.

Trennung der Netze: die internen Netze der Intus Data sind getrennt von Netzen mit Kundendiensten. Auch einzelne kundenbezogenen Dienste sind untereinander nur wo absolut nötig verbunden.

Administrativer Zugriff auf Serverressourcen ist eingeschränkt auf ein kleines Team von IT-Administratoren.

Sämtliche vorhandenen Passwörter sind nach dem "need to know" Prinzip nur für diejenigen Benutzer verfügbar, welche im entsprechenden Prozess mitarbeiten.

Physische Sicherheit an den Standorten der Intus Data AG. Büroräumlichkeiten sind permanent verschlossen und die internen Serverräumlichkeiten sind überwacht mit Kamera, Rauch- und Temperatursensoren.

Umgang mit Kundendaten (Daten im Besitz von Kunden, nicht nur, aber auch, Personendaten). In einem etablierten monatlichen Prozess werden Kundendaten (z.B. aus Supportanfragen) identifiziert und gelöscht, falls diese nicht mehr für einen Auftrag benötigt werden und falls kein Auftrag zur permanenten Speicherung vorliegt.

Passwörter von Kundensystemen werden nur gemäss separatem Kundenauftrag gespeichert. Die Speicherung erfolgt ausschliesslich im Remote Desktop Manager (devolutions) und werden nach Beendigung des Auftrags gelöscht.

11 Verarbeitung von Personendaten im internen Netzwerk

Bei einem Auftrag zur Migration von Daten oder einem Auftrag zur Speicherung einer Datenbank erfolgt die Verarbeitung im internen Netzwerk der Intus Data (LAN). Alternativ dazu kann die Migration von Daten auch auf der Infrastruktur des Kunden erfolgen.

Der Zugriff zum Intus Data LAN ist eingeschränkt für Geräte, die gemäss Abschnitt 10 geschützt sind. Fremde Geräte sind hardwaremässig vom Zugriff auf das interne LAN ausgeschlossen (kein "BYOD").

Nach Beendigung des Auftrages löscht Intus Data die Kundendaten.

12 Intus Data Cloud Abo (Treuhandportal)

Mit dem Intus Data Cloud Abo (Treuhandportal) wird die Software von Intus Data betrieben. Welche (und ob überhaupt) Personendaten mitverarbeitet werden, hängt vom konkreten Anwendungsfall des Kunden ab. Intus Data verarbeitet die Personendaten des Kunden da in Regel vollständig automatisch, eine manuelle Bearbeitung oder sogar Anreicherung erfolgt dabei nicht.

Ausnahmen sind:

Kontrolle der Funktionsweise des Backup-Systems der Datenbank durch ein Restore im Stichprobenverfahren.

Bei einem Auftrag des Kunden zur Auslieferung der Datenbank oder einem Auftrag des Kunden zum Restore.

Im Disaster Recovery Fall.

Die Cloud / SaaS Abo Infrastruktur besteht aus mehreren verbundenen Linux und Windows Servern in der Schweiz. Der administrative Zugriff ist auf diese Server vom Personenkreis her stark eingeschränkt. Die Kommunikation zwischen den Servern untereinander, von der Cloud Abo Infrastruktur zu den Client-Applikationen der Kunden sowie der administrative Zugriff erfolgt verschlüsselt.